Introduction to Application Security

Course Summary

Description

This introduction to application security is intended to provide junior web application developers with a better understanding of common attack vectors used by attackers, as well as the potential risks to their applications, and the surrounding systems.
The course provides developers with the basic security fundamentals, as well as live examples of typical programming mistakes that are made by development teams. It also shows participants how relatively simple programming mistakes can have a critical impact on a system's security.

Objectives
By the end of this course, students will be able to:

- Understand how the Web works from the perspective of an application developer
- Learn about web protocols and their weaknesses
- Learn about common developer bugs and how to avoid them
- Identify weaknesses in web applications
- Learn to develop web applications with security in mind

Topics

- Introduction to the Web
- The HTTP Protocol
- Rendering
- Isolation
- Communication
- Navigation
- Cookies
- Secure UI
- Session Management
- Frame busting
- Command Injection
- SQL Injection Attacks
- XSS Attacks
- CSRF Attacks
- Session Hijacking

Audience

Junior web application developers (including experienced developers who are new to web application development)

Prerequisites

To take this course, you must have some practical software development experience.

Duration

One day